一种抗盲检测的直扩隐蔽信号设计方法

谢岸宏[1],朱立东[1],翟继强[2],李雄飞[2]
(1. 电子科技大学通信抗干扰技术国家级重点实验室,四川成都 611731;
2. 中国空间技术研究院西安分院,陕西西安 710100)

摘 要: 直扩信号具有抗干扰抗截获能力,在电子对抗、卫星通信、测控数传等方面有重要的应用价值. 考虑到采用固定 PN 码、跳码和可变符号周期混沌序列等来提升信号抗截获能力的方式较为单一,本文将大信号掩盖技术与直扩技术结合,提出了一种增强信号隐蔽性的波形设计方法. 将不同保密级别的数据分级调制实现大信号掩盖小信号,并从功率和周期两个方面对波形参数进行设计,突出大信号参数特征,隐藏机密信号特征. 仿真表明设计的信号波形可抵抗常规盲检测,同时通过设置合理的波形参数可使机密信号的解调损失小于 0.5dB.

关键词: 通信对抗; 大信号掩盖; 抗截获; 直扩信号; 波形设计; 抗盲检测
中图分类号: TN914.42 **文献标识码:** A **文章编号:** 0372-2112 (2018)12-2817-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.12.001

A Method of Designing Covert DSSS-Signal for Anti-blind Detection

XIE An-hong[1], ZHU Li-dong[1], ZHAI Ji-qiang[2], LI Xiong-fei[2]
(1. *National Key Laboratory of Science and Technology on Communications, UESTC, Chengdu, Sichuan* 611731, *China*;
2. *China Academy of Space Technology (Xi'an), Xi'an, Shaanxi* 710100, *China*)

Abstract: DSSS-Signal (Direct Sequence Spread Spectrum Signal) has the ability of anti-jamming and anti-interception, it is widely used in electronic countermeasures, satellite communications, measurement and data transmission. It is simplex to improve signal anti-interception by the method of fixed PN (Pseudo-Noise) code, code hopping and variable symbol period chaotic sequence. Therefore, we combine the strong-signal masking technology with direct sequence spread spectrum technology, and propose a waveform design method to enhance the signal covertness. The data of different security levels are modulated hierarchically to make strong-signal mask weak-signal, also the parameters of waveform are designed in the aspects of power and period to highlight the characteristics of strong-signal and hide the confidential signal. Simulations show that the designed signal waveform can resist conventional blind detection. Moreover, setting the waveform parameters reasonably can achieve demodulation loss less than 0.5 dB.

Key words: communication countermeasure; strong-signal masking; anti-interception; direct sequence spread spectrum signal; waveform design; anti-blind detection

1 引言

直扩信号是一种传统的抗干扰抗截获信号,并在通信对抗中得到成熟运用[1]. 随着扩频信号检测技术的发展,使用固定 PN 码扩频的信号隐蔽性下降. 针对这种情况,Heidari-Bateni G 等[2]采用混沌序列替代 PN 码实现直接序列扩频,提升了信号在基于期望的盲检测技术下的抗截获能力. 雷莉等[3]设计了一个混沌跳码直接序列扩频通信系统,利用混沌序列实现跳码,进一步提升信号的抗截获能力. Nguyen Xuan Quyen 等[4]提出了一种具有可变符号周期的混沌直接序列扩频方法,对扩频码符号周期进行设计,打破基本参数周期特征,增强信号抗检测能力. 但仅通过对扩频信号本身的设计来保证抗截获性的方法较为单一,需

收稿日期:2017-11-10;修回日期:2018-02-05;责任编辑:覃怀银
基金项目:预研基金(No. 61405180503, No. 6141B062901);国家高技术研究发展计划(863 计划)(No. 2012AA01A502);四川省科技厅资助项目(No. 2014GZX004)

对信号进行多维度设计. 陈琦等[5]首次分析了大信号掩盖技术在信息安全中的应用,提出了用大信号掩盖技术来提升信号抗截获能力的基本方法. 然而其没有对相关参数进行分析设计,并且也存在大信号功率浪费的问题.

本文结合大信号掩盖技术与直扩技术,提出基于数据分级的大信号掩盖技术,并在大信号掩盖框架下,提出抗盲检测信号参数设计方案. 采用大信号掩盖微弱机密信号传输的方式设计信号波形,可以抵抗常规盲检测及多天线截获,进而提高机密信号抗截获能力. 下面将详细介绍基于数据分级的大信号掩盖技术、抗盲检测参数设计过程,分析机密信号解调损失.

2 基于数据分级的大信号掩盖技术

大信号掩盖技术是一种利用强功率、显著参数特征掩盖信道中的有用信号,增加非合作方截获有用信号的难度,保障信号抗截获性的技术. 但大信号消耗功率仅用来提升有用信号的抗截获性,导致功率浪费. 本文提出基于数据分级的大信号掩盖技术,该技术可充分利用发射端功率. 基于数据分级的大信号掩盖原理如图 1 所示.

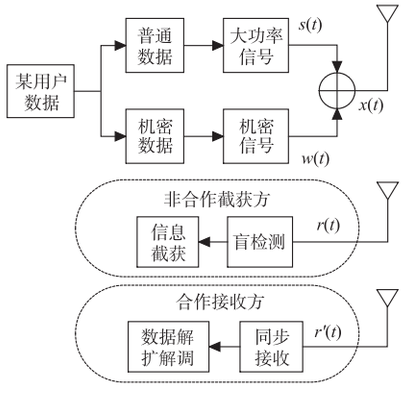


图1 基于数据分级的大信号掩盖原理框图

如图 1 将单用户数据分级为普通数据和机密数据,普通数据调制成大功率信号 $s(t)$,机密数据调制成功率较小的机密信号 $w(t)$,然后将大信号和小信号叠加发送,发送信号表示为

$$\begin{aligned} x(t) &= s(t) + w(t) \\ &= \sqrt{2P_s}m_s(t)c_s(t)\cos(2\pi f_s t) \\ &\quad + \sqrt{2P_w}m_w(t)c_w(t)\cos(2\pi f_w t) \end{aligned} \tag{1}$$

其中,P_s 和 P_w 分别为大信号和机密信号功率;信息序列波形 $m_s(t)$ 为 $\sum m_s^{(j)}q(t-jT_s)$,$m_w(t)$ 为 $\sum m_w^{(j)}q(t-jT_s)$,T_s 和 T_w 分别为大信号和机密信号的信息符号宽度,$m_s^{(j)}, m_w^{(j)} \in \{+1, -1\}$,$q(t)$ 为矩形脉冲;扩频序列波形 $c_s(t)$ 为 $\sum c_s^{(i)}q(t-iT_{sc})$,$c_w(t)$ 为 $\sum c_w^{(i)}q(t-iT_{wc})$,$T_{sc}$ 和 T_{wc} 为码片宽度,其中 $c_s^{(i)}, c_w^{(i)} \in \{+1, -1\}$;$f_s$ 和 f_w 分别为大信号和机密信号载波频率. 合作方接收到信号 $r'(t)$ 后,先进行大信号接收解调,然后自干扰抵消,最后完成机密信号的接收解调. 非合作方截获信号为 $r(t) = x(t) + n(t)$,其中 $n(t)$ 为高斯白噪声. 非合作方没有先验信息,对 $x(t)$ 中具体信号成分未知,因此,非合作方在实现机密信息截获之前,需要对 $x(t)$ 中的机密信号进行盲检测. 发射端通过对大信号和机密信号波形参数的设计,利用大信号显著参数特征掩盖机密信号,可以增加非合作方截获机密信号的难度. 大信号携带通信数据,避免功率浪费,同时掩盖机密信号,提升机密信号抗截获能力.

3 抗盲检测参数设计

3.1 功率参数设计

在强干扰下,信号检测和接收的性能会大幅下降. 相似地,采用大功率信号掩盖机密信号,大功率信号功率越强,非合作方对机密信号的盲检测性能越差,进而机密信号抗截获能力越强. 但考虑到实际应用和硬件要求,大信号功率不能无限制增大. 在获得较好的抗截获能力和合作方接收正常的前提下,需要找到功率比的最小值. 因此,提出如下的方案:

功率参数设计方案 用大信号频带完全覆盖机密信号频带,同时设计大信号和机密信号的功率参数满足 $P_s/P_w \geqslant \eta_0$,η_0 表示能够保证机密信号抗盲检测的最小功率比值.

在盲检测技术中,能量检测法[6]、文献[7]算法和平方倍频法[8]等对信号功率参数依赖性较强,其中平方倍频法对信号功率较为灵敏,具有代表性. 因此,以平方倍频法为例,对功率参数 P_s 和 P_w 进行适应性设计. 工程中常用的平方倍频法如框图 2 所示.

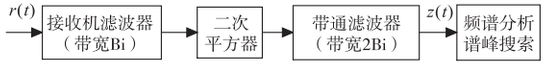


图2 平方倍频法原理

根据图 2 平方倍频法,输出信号可表示为

$$\begin{aligned} z(t) &= \sqrt{P_s P_w}m_s(t)m_w(t)c_s(t)c_w(t)\cos(2\pi(f_s+f_w)t) \\ &\quad + P_s\cos(4\pi f_s t) + P_w\cos(4\pi f_w t) + \mathrm{BPF}\{n'(t)\} \end{aligned} \tag{2}$$

其中,$t_0 \leqslant t \leqslant t_0 + \Delta t$,$n'(t) = n^2(t) + [s(t) + w(t)] \times n(t)$. 令 $d(t) = m_s(t)m_w(t)c_s(t)c_w(t)$,$d(t)$ 可进一步化简为 $\sum d_l q(t - lT_c)$,$d_l \in \{+1, -1\}$,$T_c = \min\{T_{sc}, T_{wc}\}$. 则 $z(t)$ 在频率正半轴通带范围内的频谱为

$$
\begin{aligned}
Z(f) &= \int_{t_0}^{t_0+\Delta t} z(t)\,\mathrm{e}^{-\mathrm{j}2\pi ft}\,\mathrm{d}t, f \geq 0 \\
&= \underbrace{0.5\sqrt{P_s P_w}\,\frac{\sin\{\pi[f-(f_s+f_w)]T_c\}}{\pi[f-(f_s+f_w)]}}_{V(f)} \sum_{l=\lfloor t_0/T_s \rfloor}^{\lceil (t_0+\Delta t)/T_s \rceil - 1} d_l \mathrm{e}^{-\mathrm{j}\pi[f-(f_s+f_w)](2l+1)T_c} \\
&\quad + \underbrace{0.5P_s\,\frac{\sin[\pi(f-2f_s)\Delta t]}{\pi(f-2f_s)}\mathrm{e}^{-\mathrm{j}\pi(f-2f_s)(2t_0+\Delta t)}}_{S_2(f)} \\
&\quad + \underbrace{0.5P_w\,\frac{\sin[\pi(f-2f_w)\Delta t]}{\pi(f-2f_w)}\mathrm{e}^{-\mathrm{j}\pi(f-2f_w)(2t_0+\Delta t)}}_{W_2(f)} + N'(f)
\end{aligned} \tag{3}
$$

其中,$N'(f)$对于任意的f都是一个复随机变量. 若非合作方盲检测门限为$\beta = \alpha \times \max\{|Z(f)|\}$,那么要实现机密信号在平方倍频法下的隐蔽性,则必须满足条件$|Z(2f_w)| < |Z(2f_s)|$,其中α为检测门限系数. 将式(3)带入不等式得到

$$
\begin{aligned}
&|S_2(2f_w) + 0.5P_w\Delta t + V(2f_w) + N'(2f_w)| \\
&< \alpha |W_2(2f_s) + 0.5P_s\Delta t + V(2f_s) + N'(2f_s)|
\end{aligned} \tag{4}
$$

其中,$2\pi|f_s - f_w|$远大于$|\sin[2\pi(f_s - f_w)\Delta t]|$,$\pi|f_s - f_w|$远大于$|\sin[\pi(f_s - f_w)T_c]|$,故$S_2(2f_w)$和$W_2(2f_s)$可以忽略不计. 令$V = V(2f_s) = V(2f_w)$,注意$\Delta t$数值相对较大,故不等式(4)可化简为

$$
P_s > \frac{P_w}{\alpha}\sqrt{1 + 4\left(\frac{\mathrm{Re}\{V + N'(2f_w)\}}{\Delta t P_w} + \frac{|N'(2f_w) + V|^2}{\Delta t^2 P_w^{\,2}}\right)} \tag{5}
$$

令$\gamma = [1 + 4(\mathrm{Re}\{V + N'(2f_s)\}/(\Delta t \times P_w) + |V + N'(2f_s)|^2/(\Delta t \times P_w)^2)]^{1/2}$,不等式(5)可化简为

$$
10\lg(P_s/P_w) > 10\lg(1/\alpha)\,\mathrm{dB} + 10\lg(\gamma)\,\mathrm{dB} \tag{6}
$$

在设计功率参数时,保证$10\lg(\eta_0) > 10\lg(1/\alpha)\,\mathrm{dB} + 10\lg(\gamma)\,\mathrm{dB}$,则可保证机密信号在平方倍频法下的抗盲检测能力. 后续将在仿真中分析其它几种依赖功率参数的盲检测方法对信号的盲检测情况.

3.2　扩频码周期参数设计

当非合作方采用强干扰消除技术辅助信号截获时,功率压制不能保证机密信号的抗盲检测能力. 本文提出周期参数设计方案,使机密信号在大信号残余信号下也能得到隐藏.

周期参数设计方案　扩频码周期参数设置为$T_w = mT_s$,$m = 2,3,4\cdots$;码片宽度设置为$T_{wc} = kT_{sc}$,$k = 2,3,4\cdots$. 若大信号扩频码确定,当m/k足够大时,机密信号的扩频是一种特殊情况,即机密信号采用长周期序列扩频,例如:跳码扩频和深度扩频.

当T_w和T_s、T_{wc}和T_{sc}之间构成整数倍关系时,依赖周期参数进行盲检测的输出表现为大信号成分完全掩盖弱信号成分,非合作方无法检测多个信号的存在. 即使机密信号成分的脉冲可达检测门限,非合作方也只能检测到一个恒定的脉冲间距值,这个恒定的脉冲间距与大信号的参数特征相同. 因此,在大信号被干扰消除的情况下,大信号残余依然可以保证机密信号的隐蔽性.

相关检测[9]、功率谱二次处理[10]、循环谱法[11]、高阶累积量[12]等算法,本质上都是检测扩频信号的周期性(强周期和弱周期). 以功率谱二次处理为例,验证以上方案的有效性,在后续仿真中,补充验证多个代表性算法下脉冲峰的分布情况.

功率谱二次处理是在信号功率谱的基础上进行傅里叶变换. 故在此先考虑信号的自相关函数,分析信号功率谱. 经过强干扰抵消和下变频处理后,接收信号的自相关函数为

$$
\begin{aligned}
R_y(\tau) &= R_{s'}(\tau) + R_{w'}(\tau) + N_0/2 \cdot \delta(\tau) \\
&= 2\hat{P}_s R_{m_s}(\tau) \cdot R_{c_s}(\tau) + 2P_w \cos(2\pi\Delta f\tau) \cdot R_{m_w}(\tau) \\
&\quad \cdot R_{c_w}(\tau) + N_0/2 \cdot \delta(\tau)
\end{aligned} \tag{7}
$$

其中,$\Delta f = |f_s - f_w|$. 则功率谱$S_{s'}(f)$和$S_{w'}(f)$如下所示[13]

$$
S_{s'}(f) \approx \begin{cases} \dfrac{2\hat{P}_s}{N_{cs}} \displaystyle\sum_{k=-\infty, k\neq 0}^{+\infty} S_a^{\,2}(\pi k/N_{cs})\delta(f - k/T_s), & k = 0 \\ 0, & \end{cases} \tag{8}
$$

$$
S_{w'}(f) \approx \begin{cases} \dfrac{2P_w}{N_{cw}} \displaystyle\sum_{k=-\infty, k\neq 0}^{+\infty} S_a^{\,2}(\pi k/N_{cw})\delta(f - \Delta f - k/T_w), & k = 0 \\ 0, & \end{cases} \tag{9}
$$

其中,$S_a(x) = \sin(x)/x$,N_{cs}、N_{cw}分别为大信号和机密信号的扩频码码长. 由于傅里叶变换具有线性性,接收信号的二次功率谱可表示为

$$
\begin{aligned}
\tilde{S}_y(h) &= \left|\mathrm{FT}\{\mathrm{FT}\{R_y(\tau)\}\}\right|^2 \\
&= \left|\mathrm{FT}\{S_{s'}(f)\} + \mathrm{FT}\{S_{w'}(f)\} + \mathrm{FT}\{S_n(f)\}\right|^2 \\
&\cong \left|2\hat{P}_s T_{sc} \sum_{k=-\infty}^{+\infty}\left(1 - \frac{|h - kT_s|}{T_{sc}}\right)\right|^2_{|h-kT_s| \leqslant T_{sc}, k=0,\pm1,\pm2,\cdots} \\
&\quad + \left|2P_w T_{wc} \sum_{k=-\infty}^{+\infty}\left(1 - \frac{|h - kT_w|}{T_{wc}}\right)\right|^2_{|h-kT_w| \leqslant T_{wc}, k=0,\pm1,\pm2,\cdots} \\
&\quad + N_0(2\hat{P}_s T_{sc} + 2P_w T_{wc} + N_0/4) \cdot \delta(h) + \nu(h)
\end{aligned} \tag{10}
$$

其中,$v(h)$为交叉项.$\tilde{S}_y(h)$中出现周期性三角脉冲,其脉冲中心位置为 $h=kT_s$ 和 $h=kT_w$,$k=0,\pm1,\pm2,\cdots$.当扩频码周期采用方案 $T_w=mT_s$,$m=2,3,4\cdots$时,发现 $\tilde{S}_y(h)$中三角脉冲的间隔恒为 T_s,与大信号的参数特征相同,未发现机密信号的参数特征.因此,采用所提方案设计的机密信号可以抵抗基于功率谱二次处理的盲检测.

4 解调损失分析

在大信号掩盖下,机密信号的解调必然受到影响.下面分析机密信号解调 BER(Bit Error Rate).机密信号在 $(i-1)T_w\leqslant t<iT_w$ 内的波形 $w_i(t)$可表示为$(2P_w)^{1/2}\cdot m_i c_w(t)\cos(2\pi f_w t)$,那么机密信号一个比特的能量为 $E_{\mathrm{bw}}=P_wT_w$.若 BPSK 信号采用 LPF(Low Pass Filter)基带接收,则经过机密信号解扩解调的输出信号为

$$\begin{aligned}r_i=&\underbrace{\int_{(i-1)T_w}^{iT_w}\mathrm{LPF}\{w_i(t)(c_w(t)\times2\cos(2\pi f_w t))\}\mathrm{d}t}_{r_w^{(i)}}\\&+\underbrace{\int_{(i-1)T_w}^{iT_w}\mathrm{LPF}\{s(t)(c_w(t)\times2\cos(2\pi f_w t))\}\mathrm{d}t}_{r_s^{(i)}}\\&+\underbrace{\int_{(i-1)T_w}^{iT_w}\mathrm{LPF}\{n(t)(c_w(t)\times2\cos(2\pi f_w t))\}\mathrm{d}t}_{r_n^{(i)}}\end{aligned}\tag{11}$$

当大信号不存在时,r_i 只存在 $r_w^{(i)}$ 和 $r_n^{(i)}$ 两项.$r_n^{(i)}\sim N(0,2N_0E_{\mathrm{cw}})$,其中 $E_{\mathrm{cw}}=T_w$,可得 $r_i\sim N(r_w^{(i)},2N_0T_w)$.由于 $r_w^{(i)}$ 可化简为$(2P_w)^{1/2}m_iT_w$,当 $m_i=-1$ 时,则 $r_i\sim N(-T_w(2P_w)^{1/2},2N_0T_w)$;当 $m_i=+1$ 时,则 $r_i\sim N(T_w(2P_w)^{1/2},2N_0T_w)$.信息传输中 $p(m_i=-1)$和 $p(m_i=+1)$为 0.5,系统机密信号 BER 为[14]

$$\begin{aligned}p_e=&p(m_i=-1)\cdot\int_0^{+\infty}f_r(x)\mid_{m_i=-1}\mathrm{d}x\\&+p(m_i=+1)\cdot\int_{-\infty}^{0}f_r(x)\mid_{m_i=+1}\mathrm{d}x\\=&\frac{1}{2}\left\{Q\left(\sqrt{\frac{E_{\mathrm{bw}}}{N_0}}\right)+Q\left(\sqrt{\frac{E_{\mathrm{bw}}}{N_0}}\right)\right\}\\=&Q\left(\sqrt{\frac{E_{\mathrm{bw}}}{N_0}}\right)\end{aligned}\tag{12}$$

当大信号存在时,同理可得:当 $m_i=-1$ 时,则 $r_i\sim N(r_s^{(i)}-T_w(2P_w)^{1/2},2N_0T_w)$;当 $m_i=+1$ 时,则 $r_i\sim N(r_s^{(i)}+T_w(2P_w)^{1/2},2N_0T_w)$.根据式(1)和式(11),$r_s^{(i)}$化简为

$$r_s^{(i)}=\sqrt{2P_s}\int_{(i-1)T_w}^{iT_w}\mathrm{LPF}\{m_s(t)c_s(t)c_w(t)\cos(2\pi\Delta ft)\}\mathrm{d}t\tag{13}$$

令 $\mu_s^{(i)}=1/T_w\times\int_{(i-1)T_w}^{iT_w}\mathrm{LPF}\{m_s(t)c_s(t)c_w(t)\cdot\cos(2\pi\Delta ft)\}\mathrm{d}t$,$\eta=P_s/P_w$,则 $r_s^{(i)}=\mu_s^{(i)}T_w(2\eta P_w)^{1/2}$.机密信号第 i 个数据符号的错误概率为

$$\begin{aligned}p_e^{(i)}=&\frac{1}{2}Q\left(\sqrt{\frac{E_{\mathrm{bw}}}{N_0}}(1-u_s^{(i)}\sqrt{\eta})\right)\\&+\frac{1}{2}Q\left(\sqrt{\frac{E_{\mathrm{bw}}}{N_0}}(1+u_s^{(i)}\sqrt{\eta})\right)\end{aligned}\tag{14}$$

当信号参数确定时,在$[(i-1)T_w,iT_w]$内的大信号数据 $m_s^{(j)}$ 的随机性导致了 $\mu_s^{(i)}$ 具有随机性.其中,m_s 序列有 $2^{T_w/T_s}$种可能,m_s 的有限性决定了 $\mu_s^{(i)}$ 的随机取值集合 Ω 的有限性.当 T_w/T_s 较大时,Ω 中元素虽然较多,但具有有限性,可以利用计算机蒙特卡洛仿真实验来分析具体信号波形相应的理论 p_e,如下所示

$$p_e=\lim_{L\to\infty}\frac{1}{L}\sum_{i=1}^{L}p_e^{(i)}\tag{15}$$

其中,L 表示样本数.由于计算机仿真数据样本有限,当 $L\geqslant100|\Omega|$时,仿真的 BER 值具有参考意义.另外,根据式(14)可以看出,机密信号的 BER 和 E_{bw}/N_0、μ_s、η 有关.在仿真实验中将具体分析这些参数对机密信号解调损失的影响.

5 仿真实验

实验 1 仿真中大信号相关参数设置为:$1/T_s=38.4\mathrm{kbps}$,$N_{\mathrm{cs}}=32$,$T_{\mathrm{sc}}=1.2288\mathrm{Mcps}$,$f_s=90.8304\mathrm{MHz}$;机密信号相关参数设置为:$1/T_w=19.2\mathrm{kbps}$,$N_{\mathrm{cw}}=64$,$T_{\mathrm{wc}}=1.2288\mathrm{Mcps}$,$f_w=90.95328\mathrm{MHz}$.信噪比 SNR 为机密信号相对白噪声的比值,采样率为 908.304MHz.

图 3 是平方倍频法(门限系数 $\alpha=0.1$)、能量检测法和文献[7]方法对机密信号的盲检测概率的仿真情况,图中能量检测法在有大信号存在的情况下基本失效,文献[7]方法本质上有一个强干扰抵消的过程,所以对机密信号盲检测效果最好,但是当 P_s/P_w 大于 16dB 时,却不能检测到机密信号.因此,$10\lg(\eta_0)=$

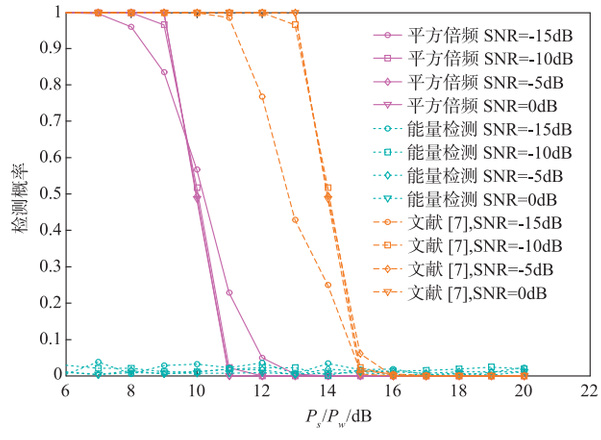
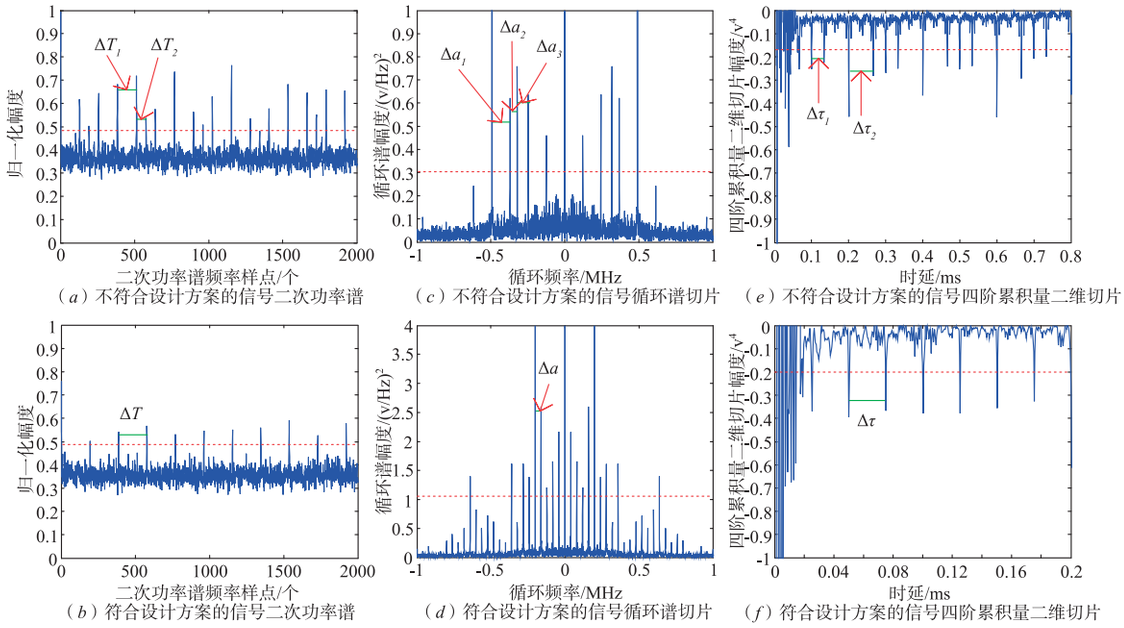


图3 依赖功率参数的机密信号盲检测概率

16dB 是一个可靠的参数,因此前文的功率参数设计方案在满足 $P_s/P_w \geqslant 16$dB 时,可以保证机密信号的抗盲检测能力.

实验 2　仿真中设置 $T_w = 1.5T_s$ 和 $T_{wc} = 1.5T_{sc}$,盲检测算法对接收信号的处理输出如图 4(*a*)、4(*c*)、4(*e*)所示. 再考虑 $T_w = 4T_s$ 和 $T_{wc} = 2T_{sc}$(满足前文提出的周期参数设计方案),盲检测算法对接收信号的处理输出如图 4(*b*)、4(*d*)、4(*f*)所示.



(*a*) 不符合设计方案的信号二次功率谱　(*c*) 不符合设计方案的信号循环谱切片　(*e*) 不符合设计方案的信号四阶累积量二维切片

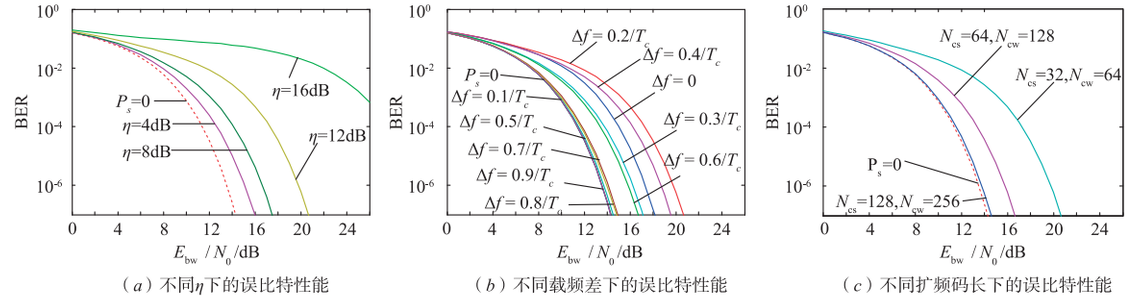
(*b*) 符合设计方案的信号二次功率谱　(*d*) 符合设计方案的信号循环谱切片　(*f*) 符合设计方案的信号四阶累积量二维切片

图4　依赖周期参数的机密信号盲检测

图 4(*a*)和图 4(*b*)为二次功率谱盲检测输出,图 4(*c*)和图 4(*d*)为循环谱检测法频率为 0Hz 时的盲检测输出,图 4(*e*)和图 4(*f*)为四阶累积量盲检测法的四阶累积量二维切片输出. 图 4(*a*)、4(*c*)、4(*e*)中输出谱峰均存在多间隔值现象,此现象将导致非合作方检测到接收信号中信号成分不唯一,除大信号残留外还存在其它信号,进而机密信号的隐蔽性降低;图 4(*b*)、4(*d*)、4(*f*)中输出谱峰的间隔均为唯一值,且参数特性符合大信号参数特征,机密信号得到隐藏,具有抗盲检测能力.

实验 3　仿真讨论大信号掩盖下不同参数对机密信号解调损失的影响. 仿真中信号均采用 BPSK 调制方式,E_{bw}/N_0取 0dB ~ 26dB,$L = 10^5$. 机密信号 BER 理论值如图 5 所示.

图 5(*a*)是不同 P_s/P_w 下机密信号盲解调 BER 的理论值,Δf 为 $0.2/T_c$,N_{cs} 和 N_{cw} 分别为 32、64. 大信号功率越大,机密信号的 BER 越高,解调增益损失越大. 当 P_s/P_w 为 16dB、机密信号的 BER 达 10^{-7} 时,解调损失超过 12dB. 因此,合作方在接收前进行大信号自干扰抵消处理是必要的. 图 5(*b*)是不同载频差 Δf 下机密信号解调 BER 的理论值,P_s/P_w 取 12dB,N_{cs} 和 N_{cw} 分别为 32、64. 图中 $\Delta f = 0.2/T_c$ 机密信号解调性能最差,可见解调



(*a*) 不同η下的误比特性能　(*b*) 不同载频差下的误比特性能　(*c*) 不同扩频码长下的误比特性能

图5　大信号掩盖下机密信号解调BER理论值

BER 并不是 Δf 的单调函数,但是随着 Δf 增大,解调 BER 大体呈下降趋势. 图 5(c)是不同扩频码长下机密信号的解调 BER 理论值,P_s/P_w 取 12dB,Δf 取 $0.2/T_c$. 图中大信号和机密信号选取的扩频码的码长越长,机密信号解调损失越小. 当 $N_{cs}=32$、$N_{cw}=64$、机密信号 BER 达 10^{-7} 时,大信号带来的机密信号解调损失为 6dB 左右. 但当 $N_{cs}=128$、$N_{cw}=256$ 时,大信号带来的机密信号解调损失低于 0.5dB. 可见扩频码码长对解调损失影响巨大.

6 结论

本文提出一种抗盲检测直扩隐蔽信号设计方法,提出基于数据分级的大信号掩盖技术,给出了波形参数设计方案,并对大信号掩盖下的机密信号解调 BER 的理论值进行推导. 最后仿真验证了所提方案可实现机密信号的抗盲检测. 同时在保证机密信号抗盲检测能力的情况下,解调损失可控制在接受范围内. 未来工作将分析初始相位、扩频码等参数对信号抗截获的影响.

参考文献

[1] Fang W, Li F, Sun Y, et al. Information security of PHY layer in wireless networks[J]. Journal of Sensors, 2016, 2016(3):1 – 10.

[2] Heidari-Bateni G, Mcgillem C D. Chaotic sequences for spread spectrum: an alternative to PN-sequences[A]. Proceedings of 1992 IEEE International Conference on Selected Topics in Wireless Communications[C]. Canada: IEEE Press, 1992. 437 – 440.

[3] 雷莉,郑建生,刘郑,等. 混沌跳码扩频通信系统及其抗干扰性能分析[J]. 科学技术与工程,2014,14(30):176 – 180.
Lei Li, Zheng Jian-sheng, Liu Zheng. The chaotic code-hopping spread spectrum communication system[J]. Science Technology & Engineering, 2014, 14(30):176 – 180. (in Chinese)

[4] Quyen N X, Duong T Q, Vo N S, et al. Chaotic direct-sequence spread-spectrum with variable symbol period: A technique for enhancing physical layer security[J]. Computer Networks, 2016, 109:4 – 12.

[5] 陈琦,李伟. 大信号掩盖技术在信息安全中的应用[J]. 电信快报,2014,(5):1006 – 1339.
Chen Qi, Li Wei. The technology of strong signal masking application in information security[J]. Telecommunications Information, 2014, (5):1006 – 1339. (in Chinese)

[6] Lehtomaki J J, Juntti M, Saarnisaari H. CFAR strategies for channelized radiometer[J]. IEEE Signal Processing Letters, 2005, 12(1):13 – 16.

[7] 廖灿辉,周世东,朱中梁. 从强信号掩盖中检出弱信号的一种新检测算法[J]. 系统仿真学报,2010,22(4):986 – 990.
Liao Can-hui, Zhou Shi-dong, Zhu Zhong-liang. Novel algorithm for activity detection of weak signals covered by strong signal[J]. Journal of System Simulation, 2010, 22(4):986 – 990. (in Chinese)

[8] Hill D A, Bodie J B. Carrier detection of PSK signals[J]. IEEE Transactions on Communications, 2001, 49(49):487 – 496.

[9] Zhang T, Qian W, Zhang G, et al. Parameter estimation of MC-CDMA signals based on modified cyclic autocorrelation[J]. Digital Signal Processing, 2016, 54(C):46 – 53.

[10] 张天骐,周正中. 低信噪比直扩信号伪码周期检测的谱方法[J]. 仪器仪表学报,2001,22(z2):41 – 42.
Zhang Tian-qi, Zhou Zheng-zhong. A new method of spectra for periodic detection and estimation of the PN sequence in the lower SNR DS/SS signals[J]. Chinese Journal of Scientific Instrument, 2001, 22(z2):41 – 42. (in Chinese)

[11] Damodaram D, Venkateswarlu T. Performance analysis of cyclostationary detector using efficient hardware architecture[A]. 2016 International Conference on Communication and Signal Processing[C]. India: IEEE Press, 2016. 0187 – 0193.

[12] Guan M, Wang L. A novel recognition method for low SNR DSSS signals based on four-order cumulant and eigenvalue analysis[J]. Chinese Journal of Electronics, 2015, 24(3):650 – 653.

[13] 张天骐,代少升,杨柳飞,等. 在残余频偏下微弱直扩信号伪码周期的谱检测[J]. 系统工程与电子技术,2009,31(4):777 – 781.
Zhang Tian-qi, Dai Shao-sheng, Yang Liu-fei, et al. Method of spectra for periodic detection of the PN sequence in the weak DS-SS signals with residual carrier[J]. Systems Engineering and Electronics, 2009, 31(4):777 – 781. (in Chinese)

[14] 郭黎利,李清伟,戴佳,等. 频谱重叠度对扩频通信的性能影响分析[J]. 北京邮电大学学报,2015,(6):115 – 119.
Guo Li-li, Li Qing-wei, Dai Jia, et al. The performance analysis of spectrum overlap degree impacting to spread-spectrum system[J]. Journal of Beijing University of Posts and Telecommunications, 2015, (6):115 – 119. (in Chinese)

作者简介

谢岸宏　男,1993 年生于四川攀枝花. 现为电子科技大学通信抗干扰技术国家级重点实验室硕士研究生. 主要研究方向为盲信号分离、抗干扰抗截获技术.
E-mail:yueslyun@163.com

朱立东　男,1968 年生于四川邻水. 现为电子科技大学教授、博士生导师. 主要研究方向为卫星通信信号处理、信道建模与仿真、资源管理等.
E-mail:zld@uestc.edu.cn

翟继强　男,1985 年生于河南新乡. 现为中国空间技术研究院西安分院工程师. 主要研究方向为卫星通信.
E-mail:zhaijiq@163.com

李雄飞　男,1979 年生于陕西榆林. 现为中国空间技术研究院西安分院工程师. 主要研究方向为卫星通信.
E-mail:lxf_li@163.com